Vereinbarung zwischen dem Verantwortlichen
und
dem Auftragsverarbeiter

Zwischen

Name1
Name2
Str., Hsnr.
12345 Ort
EKP-Nr. 1234567890

(im Folgenden **Verantwortlicher**)

und

Deutsche Post AG
Charles-de-Gaulle-Str. 20
53113 Bonn

(im Folgenden **DPAG**)

und

Deutsche Post E-POST Solutions GmbH
Vorgebirgsstraße 49
53119 Bonn

(im Folgenden **DPEPS**)

(DPAG und DPEPS zusammen „die Auftragsverarbeiter“)

wird folgende Vereinbarung geschlossen:

Stand der Vereinbarung

16.10.2023

MUSTER

1. Gegenstand/Umfang der Verarbeitung

(1) Gegenstand dieser Vereinbarung ist die Herstellung von digital eingelieferten Sendungen mit klassischer Briefzustellung durch die DPEPS gemäß den durch den Verantwortlichen ausgewählten Leistungen und Anbindungsvarianten, sowie den weiteren in den Allgemeinen Geschäftsbedingungen hybride Kommunikation für Geschäftskunden genannten Bedingungen, sowie den Datenschutzhinweisen für die Nutzung der digitalen und hybriden Dienste (Geschäftskunden).

(2) Gegenstand dieser Vereinbarung sind die ausgewählten Leistungen und Anbindungsvarianten aus den Anbindungsvereinbarungen, sowie die weiteren in den Allgemeinen Geschäftsbedingungen digitale Kommunikation für Geschäftskunden genannten Bedingungen, sowie den Datenschutzhinweisen für die Nutzung der digitalen und hybriden Dienste (Geschäftskunden).

2. Laufzeit

Die Laufzeit dieser Vereinbarung entspricht der Laufzeit der jeweiligen Vereinbarung zur Anbindung an das E-POST System durch die Deutsche Post E-Post Solutions GmbH („DPEPS“) nach den Allgemeinen Geschäftsbedingungen hybride Kommunikation für Geschäftskunden und die Nutzung der durch die DPAG über das E-POST System angebotenen digitalen Dienste gemäß den Allgemeinen Geschäftsbedingungen digitale Kommunikation für Geschäftskunden.

3. Spezifikationen der Verarbeitung

(1) Ort der Verarbeitung

Die Verarbeitung der vom Verantwortlichen eingelieferten Daten durch die Auftragsverarbeiter findet ausschließlich im europäischen Rechtsraum statt.

(2) Art und Zweck der beabsichtigten Verarbeitung

Art und Zweck der Verarbeitung personenbezogener Daten im Auftrag des Verantwortlichen sind in der Anbindungsvereinbarung festgelegt.

(3) Arten von Daten

Der Gegenstand der Verarbeitung personenbezogener Daten beinhaltet die folgenden Arten/Kategorien von Daten (Auflistung/Beschreibung der Datenkategorien):

- ☐ Name
- ☐ Kontaktdaten
- ☐ Vertragsdaten
- ☐ Kundenhistorie

MUSTER

- ☐ Vertragsabrechnungs- und Zahlungsverkehrsdaten
- ☐ Position/Funktion
- ☐ Besondere Kategorien personenbezogener Daten (z.B. Gesundheit, Familienstand, Gewerkschaftszugehörigkeit, politische Meinung, Rasse und ethnische Herkunft, religiöse oder weltanschauliche Überzeugung/strafrechtliche Verurteilung, genetische oder biometrische Daten)
- ☐ Bankverbindungen oder Kreditkartendaten

(4) Betroffene Person

Die Kategorien von betroffenen Personen beinhalten:

- ☐ Kunden
- ☐ Potenzielle Kunden/interessierte Kreise
- ☐ Mitarbeiter
- ☐ Auftragsverarbeiter
- ☐ Ansprechpartner

4. Technische und organisatorische Maßnahmen

(1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen sind die Auftragsverarbeiter verpflichtet, geeignete technische und organisatorische Maßnahmen zu treffen, und zwar auf eine Art und Weise, dass die Verarbeitung personenbezogener Daten die Anforderungen des anwendbaren Datenschutzrechts, insbesondere der DSGVO und dieser Vereinbarung, erfüllt. Die Auftragsverarbeiter erkennen hiermit die Rechte der betroffenen Personen, wie vorstehend angegeben, an und gewährleisten diese. Zu diesem Zweck und nach Maßgabe von Artikel 32 DSGVO haben die Auftragsverarbeiter die spezifischen Maßnahmen angemessen zu dokumentieren und dem Verantwortlichen zur Genehmigung vorzulegen. Nach einvernehmlicher Vereinbarung werden die technischen und organisatorischen Maßnahmen integraler Bestandteil der Vereinbarung.

(2) Die vorzunehmenden Maßnahmen sind Maßnahmen der Datensicherheit und Maßnahmen, die ein angemessenes Schutzniveau in Bezug auf das Risiko betreffend Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme gewährleisten. Stand der Technik, Implementierungskosten, Art, Umfang und Zwecke der Verarbeitung sowie Eintrittswahrscheinlichkeit und Schwere eines Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Artikel 32 Absatz 1 DSGVO sind zu berücksichtigen.

(3) Die technischen und organisatorischen Maßnahmen ändern sich mit dem technischen Fortschritt und werden beständig weiterentwickelt. In diesem Zusammenhang können die Auf-

MUSTER

tragsverarbeiter geeignete alternative Maßnahmen ergreifen. Das Sicherheitsniveau der genannten Maßnahmen darf jedoch nicht unter das in dieser Vereinbarung vereinbarte Niveau sinken.

(4) Daher und nach Maßgabe dieser Ziffer 4 bestätigen die Auftragsverarbeiter hiermit die Umsetzung der technischen und organisatorischen Maßnahmen, wie in Anlage 1 dieser Vereinbarung angegeben und ausgeführt.

(5) Unbeschadet des Vorstehenden haben die Auftragsverarbeiter ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen einzuführen, um die in dieser Vereinbarung vereinbarte Sicherheit der Verarbeitung zu gewährleisten.

5. Berichtigung, Einschränkung und Löschung von Daten

(1) Die Auftragsverarbeiter dürfen personenbezogene Daten nur auf Weisung des Verantwortlichen berichtigen, löschen oder sperren. Beantragt eine betroffene Person die Berichtigung oder Löschung direkt bei den Auftragsverarbeitern, haben die Auftragsverarbeiter diesen Antrag unverzüglich an den Verantwortlichen weiterzuleiten.

(2) Die Auftragsverarbeiter haben den Verantwortlichen nach Möglichkeit bei der Erfüllung der Pflicht des Verantwortlichen zur Beantwortung von Anträgen auf Wahrnehmung der Rechte der betroffenen Person zu unterstützen. Zu diesen Rechten zählen das „Recht auf Vergessenwerden“ sowie die Rechte auf Berichtigung, Datenübertragbarkeit und Auskunft.

(3) Die Auftragsverarbeiter haften nicht dafür, dass der Antrag einer betroffenen Person nicht, nicht korrekt oder nicht rechtzeitig seitens des Verantwortlichen beantwortet worden ist.

6. Pflichten der Auftragsverarbeiter

Neben den in dieser Vereinbarung enthaltenen Regelungen und Pflichten haben die Auftragsverarbeiter die gesetzlichen Vorschriften nach Artikel 28–33 DSGVO zu beachten. Dies vorausgeschickt, verpflichten sich die Auftragsverarbeiter insbesondere dazu,

(1) personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen zu verarbeiten, sofern die nicht durch das anwendbare Recht, dem die Auftragsverarbeiter unterliegen, hierzu verpflichtet sind; in einem solchen Fall teilen die Auftragsverarbeiter, sofern gesetzlich gestattet, dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung der personenbezogenen Daten mit. Die Auftragsverarbeiter haben mündliche Weisungen unverzüglich schriftlich oder per E-Mail zu bestätigen.

(2) den Verantwortlichen unverzüglich in Kenntnis zu setzen, wenn sie der Auffassung sind, dass eine Weisung gegen geltendes Datenschutzrecht oder -vorschriften verstößt. In diesem Fall sind die Auftragsverarbeiter berechtigt, die Ausübung der jeweiligen Weisungen auszusetzen, bis der Verantwortliche diese bestätigt oder ändert.

MUSTER

(3) einen Datenschutzbeauftragten zu ernennen oder, falls er nicht zur Ernennung eines Datenschutzbeauftragten verpflichtet ist, einen sonstigen Ansprechpartner zu ernennen, der für Fragen des Datenschutzes verantwortlich zeichnet. Die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen verantwortlichen Person sind dem Verantwortlichen mitzuteilen, damit dieser direkt Kontakt aufnehmen kann. Der Verantwortliche ist über etwaige diesbezügliche Änderungen unverzüglich in Kenntnis zu setzen. Für die DPAG und die DPEPS ist als Datenschutzbeauftragte Frau Gabriela Krader bestellt. Kontakt unter:

Deutsche Post AG
Datenschutzbeauftragte
Frau Gabriela Krader, LL.M.
53250 Bonn
Email: datenschutz@dpdhl.com

(4) ein Verzeichnis aller Verarbeitungstätigkeiten zu führen.

(5) Zugang zu den personenbezogenen Daten nur zu gewähren, wenn und soweit dieser Zugang für die Erbringung der Dienstleistungen vorgeschrieben und erforderlich ist und sofern die entsprechenden Mitarbeiter und Berater angemessene Vertraulichkeitsvereinbarungen unterzeichnet und sich zur Vertraulichkeit verpflichtet haben.

Die Auftragsverarbeiter und jede den Auftragsverarbeitern und/oder dem Verantwortlichen unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich auf Weisung des Verantwortlichen verarbeiten, es sei denn, dass sie rechtlich zur Verarbeitung verpflichtet sind.

(6) den Verantwortlichen unverzüglich über Prüfungen, Untersuchungen und/oder Verwaltungsmaßnahmen seitens einer Aufsichtsbehörde in Kenntnis zu setzen, soweit sie den Gegenstand diese Vereinbarung betreffen und dies rechtlich zulässig ist.

(7) falls der Verantwortliche Gegenstand einer Untersuchung der Aufsichtsbehörde, eines Verfahrens wegen Ordnungswidrigkeiten oder eines Strafverfahrens, eines Haftungsanspruchs seitens einer betroffenen Person oder eines Dritten bzw. eines sonstigen Anspruchs in Verbindung mit dieser Vereinbarung und der Datenverarbeitung durch die Auftragsverarbeiter wird, sich nach Kräften zu bemühen, den Verantwortlichen zu unterstützen.

(8) den Verantwortlichen so bald wie möglich über etwaige Beschwerden, Anträge bzw. Ersuchen oder sonstige Mitteilungen von betroffenen Personen, Datenschutzbehörden oder Dritten in Verbindung mit der Verarbeitung personenbezogener Daten durch die Auftragsverarbeiter und/oder den Verantwortlichen in Kenntnis zu setzen. Sofern der Verantwortliche nach geltendem Datenschutzrecht verpflichtet ist, auf einen Antrag einer betroffenen Person in Verbindung mit der Verarbeitung der Daten dieser betroffenen Person zu antworten, haben die Auftragsverarbeiter den Verantwortlichen bei der Übermittlung der verlangten Informationen zu unterstützen. Allerdings haben die Auftragsverarbeiter nicht direkt auf Anträge betroffener Personen zu antworten, sondern diese betroffenen Personen an den Verantwortlichen zu verweisen.

MUSTER

7. Unterbeauftragung

(1) Falls der Auftragsverarbeiter im Namen des Verantwortlichen einen weiteren Auftragsverarbeiter mit bestimmten Verarbeitungstätigkeiten beauftragt, werden diesem weiteren Auftragsverarbeiter im Wege einer schriftlichen Vereinbarung dieselben Pflichten wie in dieser Vereinbarung auferlegt.

(2) Auf der Grundlage der in dieser Ziffer enthaltenen Bestimmungen erteilt der Verantwortliche seine Zustimmung zu dem/den folgenden weiteren Auftragsverarbeiter(n):

Unterauftragnehmer durch DPEPS
Dienstleistung: Druck und Kuvertierung
Allianz Technology SE Königinstraße 28 80802 München
DATEV eG Paumgartnerstr. 6 – 14 90429 Nürnberg
FP Digital Business Solutions GmbH Barbara-McClintock-Straße 11 12489 Berlin
Computershare Communication Services GmbH Hansastr. 15b 80686 München
Daten-Partner Gesellschaft für Direktmarketing und Informations-Technologie mbH Feldheider Str. 39 – 45 40699 Erkrath
msp Druck und Medien GmbH Stahlwerkstraße 36 57555 Mudersbach
SDV Direct World GmbH Tharandter Straße 23–35 01159 Dresden
Schwäbisch Hall Facility Management GmbH Crailsheimer Str. 52 74523 Schwäbisch Hall
Atruvia AG Fiduciastraße 20 76227 Karlsruhe

Dienstleistung: Bereitstellen der Connext Cube und docuguide Umgebung
Formware GmbH Stangenreiter Str. 2 83131 Nußdorf am Inn

Unterauftragnehmer durch DPAG
Dienstleistung: Betrieb und Wartung der E-POST Plattform
Deutsche Post IT Services (Berlin) GmbH Ehrenbergstraße 11-14 10245 Berlin
Dienstleistung: IT Servicepartner
msg systems AG Robert-Bürkle-Str. 1 85737 Ismaning
Binect GmbH Brunnenweg 17 64331 Weiterstadt
T-Systems international GmbH Hahnstraße 43 d 60528 Frankfurt
Microsoft Ireland Operations Limited One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Irland
Noris Networks AG Thomas-Mann-Str. 16-20 90471 Nürnberg
Dienstleistung: Bereitstellen der Connext Cube und docuguide Umgebung
Formware GmbH Stangenreiter Str. 2 83131 Nußdorf am Inn

(3) Der Auftragsverarbeiter hat dem Verantwortlichen rechtzeitig mit angemessener (schriftlich oder per E-Mail erfolgter) Vorankündigung über einen neuen weiteren Auftragsverarbeiter (einschließlich der vollständigen Angaben zu der von dem neuen Auftragsverarbeiter vorgenommenen Verarbeitung) oder über Änderungen der bestehenden Liste der weiteren Auftragsverarbeiter in Kenntnis zu setzen.

(4) Bevor ein weiterer Auftragsverarbeiter zum ersten Mal personenbezogene Daten des Verantwortlichen verarbeitet, hat der Auftragsverarbeiter eine angemessene Due-Diligence-Prüfung durchzuführen, um sicherzustellen, dass der weitere Auftragsverarbeiter in der Lage ist, das in dieser Vereinbarung, dem Dienstleistungsvertrag und nach anwendbarem Recht vorgeschriebene Schutzniveau für die personenbezogenen Daten des Verantwortlichen zu bieten.

(5) Hat der Verantwortliche berechtigte Einwendungen gegen den Einsatz eines weiteren Auftragsverarbeiters durch den Auftragsverarbeiter, hat der Verantwortliche dies dem Auftragsverarbeiter umgehend schriftlich innerhalb von 10 Werktagen nach Zugang der Mitteilung des Auftragsverarbeiters mitzuteilen. Zur Klarstellung: Die Parteien vereinbaren, dass Einwendungen des Verantwortlichen nicht berechtigt sind, wenn der weitere Auftragsverarbeiter der Sicherheitsprüfung für Lieferanten des Auftragsverarbeiters standgehalten hat – es sei denn, der Verantwortliche kann nachweisen, dass der neue Auftragsverarbeiter ein unangemessenes Risiko für den Schutz personenbezogener Daten darstellt (z. B. wenn der weitere Auftragsverarbeiter in der Vergangenheit gegen Sicherheitsbestimmungen verstoßen hat) oder ein Wettbewerber des Verantwortlichen ist.

(6) Unbeschadet des Vorstehenden kommen die Parteien bei Einwendungen des Verantwortlichen gegen die Beauftragung eines weiteren Auftragsverarbeiters zusammen, um nach Treu und Glauben über eine geeignete Lösung zu beraten. Der Auftragsverarbeiter kann insbesondere beschließen, (i) den vorgesehenen Auftragsverarbeiter nicht einzusetzen oder (ii) von dem Verantwortlichen verlangte Korrekturmaßnahmen zu ergreifen und den Auftragsverarbeiter zu beauftragen. Ist keine genannte oder sonstige Option vernünftigerweise durchführbar und hat der Verantwortliche nach wie vor berechtigte Einwendungen, können beide Parteien diese Vereinbarung mit einer Frist von 10 Tagen schriftlich kündigen.

(7) Sofern und soweit ausgelagerte Nebendienstleistungen betroffen sind, ist der Auftragsverarbeiter verpflichtet, angemessene und rechtsverbindliche vertragliche Vereinbarungen abzuschließen sowie angemessene Kontrollmaßnahmen zu ergreifen, um adäquate Maßnahmen für den Schutz und die Sicherheit der Daten des Verantwortlichen zu gewährleisten.

8. Prüfrechte

(1) Nach angemessener Vorankündigung von mindestens 21 Tagen seitens des Verantwortlichen und um die Einhaltung der technischen und organisatorischen Sicherheitsmaßnahmen sowie der aus dieser Vereinbarung erwachsenden Pflichten sicherzustellen und zu überprüfen, haben die Auftragsverarbeiter dem Verantwortlichen oder einem von dem Verantwortlichen beauftragten Prüfer die Durchführung regelmäßiger Prüfungen zu gestatten, wenn

(a) der Verantwortliche die begründete Vermutung hat, dass der Auftragsverarbeiter nicht im Einklang mit den technisch-organisatorischen Maßnahmen und / oder den Verpflichtungen aus dieser Vereinbarung handelt;

(b) sich ein Sicherheitsvorfall ereignet hat;

(c) eine solche Prüfung durch die für den Verantwortlichen zuständige Aufsichtsbehörde gefordert wird.

(2) Ungeachtet des Vorstehenden kann der Nachweis für die Einhaltung der Vorschriften folgendermaßen erbracht werden:

(a) Einhaltung der genehmigten Verhaltensregeln und/oder

MUSTER

(b) Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Artikel 42 DSGVO und/oder

(c) aktuelle Zertifikate von Prüfern, Berichte oder Auszüge aus Berichten unabhängiger Stellen. Auf Verlangen des Verantwortlichen wird der Auftragsverarbeiter dem Verantwortlichen die Prüfungsberichte in den Räumen des Auftragsverarbeiters die Einsichtnahme ermöglichen, sodass der Verantwortliche angemessen überprüfen kann, ob die Auftragsverarbeiter die technischen und organisatorischen Maßnahmen und Pflichten im Rahmen dieser Vereinbarung umsetzen bzw. erfüllen.

(3) Prüfungen werden zu den üblichen Geschäftszeiten, in angemessenem Umfang und ohne Störung des Betriebsablaufs durchgeführt. Für den Fall, dass der Verantwortliche die Prüfung durch einen von ihm beauftragten unabhängigen Prüfer durchführen lässt, hat dieser zuvor eine Verschwiegenheitserklärung zu unterzeichnen. Zudem darf der unabhängige Prüfer nicht in einem Wettbewerbsverhältnis zu den Auftragsverarbeitern stehen.

Sofern die Prüfung seitens der Auftragsverarbeiter oder eines anderen Auftragsverarbeiters Aufwendungen bedeutet, die über einen Arbeitstag hinausgehen, ist der Verantwortliche damit einverstanden, jeden darüber hinaus gehenden Tag zu erstatten, es sei denn,

(a) der Verantwortliche hat die begründete Vermutung, dass die Auftragsverarbeiter nicht im Einklang mit den technisch-organisatorischen Maßnahmen und / oder den Verpflichtungen aus diesem Vertrag handeln;

(b) ein Sicherheitsvorfall hat sich ereignet;

(c) eine solche Prüfung wird durch die für den Verantwortlichen zuständige Aufsichtsbehörde gefordert.

9. Unterstützungspflichten

(1) Die Auftragsverarbeiter haben den Verantwortlichen bei der Erfüllung der Pflichten betreffend die Sicherheit personenbezogener Daten, die Meldepflichten bei Verletzungen des Schutzes personenbezogener Daten, die Datenschutz-Folgenabschätzungen und vorherige Konsultationen nach Maßgabe von Artikel 33 bis 36 DSGVO zu unterstützen. Dies umfasst insbesondere

(a) die Pflicht, eine Verletzung des Schutzes personenbezogener Daten unverzüglich dem Verantwortlichen zu melden.

(b) die Pflicht, den Verantwortlichen im Hinblick auf die Pflicht des Verantwortlichen zur Bereitstellung von Informationen zur betroffenen Person zu unterstützen und dem Verantwortlichen unverzüglich sämtliche relevanten Informationen zur Verfügung zu stellen.

(c) die Unterstützung des Verantwortlichen bei einer Datenschutz-Folgenabschätzung.

(d) die Unterstützung des Verantwortlichen in Bezug auf das Verzeichnis der Verarbeitungstätigkeiten.

MUSTER

(e) die Unterstützung des Verantwortlichen in Bezug auf die Konsultation der Aufsichtsbehörde.

(2) Dier Auftragsverarbeiter können für die unter Absatz 1 lit. (c) and (d) genannten Unterstützungsleistungen Ersatz verlangen.

10. Löschung und Rückgabe personenbezogener Daten

(1) Nach Abschluss der Auftragsarbeiten oder vorher auf Verlangen des Verantwortlichen, jedoch spätestens bei Beendigung des Dienstleistungsvertrags, haben die Auftragsverarbeiter dem Verantwortlichen sämtliche Dokumente, Verarbeitungs- und Nutzungsergebnisse sowie Datensätze im Zusammenhang mit dem Vertrag, die in seinen Besitz gelangt sind, nach Maßgabe der datenschutzrechtlichen Vorschriften auszuhändigen oder – nach vorheriger Zustimmung – zu zerstören. Gleiches gilt für Testdaten, Datenmüll sowie überflüssiges und verworfenes Datenmaterial. Das Protokoll zur Zerstörung oder Löschung ist auf Verlangen vorzuzeigen.

(2) Unterlagen, die als Nachweis für die ordnungsgemäße Datenverarbeitung dienen, sind von den Auftragsverarbeitern gemäß den entsprechenden Speicherbestimmungen aufzubewahren. Die Auftragsverarbeiter können sie dem Verantwortlichen nach Beendigung der Dienstleistung aushändigen, um von ihren diesbezüglichen Pflichten befreit zu werden.

11. Schlussbestimmungen

(1) Eine Änderung oder Ergänzung dieses Vertrags kann in Schriftform oder in elektronischer Form durch ordnungsgemäß bevollmächtigte Vertreter beider Parteien erfolgen.

(2) Werden Daten des Verantwortlichen Gegenstand einer Durchsuchung und Beschlagnahme, eines Pfändungsbeschlusses, einer Einziehung im Rahmen eines Konkurs- oder Insolvenzverfahrens bzw. ähnlicher Ereignisse oder Maßnahmen Dritter, während sie im Verantwortungsbereich der Auftragsverarbeiter sind, so haben die Auftragsverarbeiter den Verantwortlichen hierüber unverzüglich in Kenntnis zu setzen. Die Auftragsverarbeiter hat sämtlichen Beteiligten dieser Maßnahme unverzüglich mitzuteilen, dass sich hiervon betroffene Daten ausschließlich im Eigentum des Verantwortlichen befinden und in dessen Verantwortungsbereich liegen, dass der Verantwortliche das alleinige Verfügungsrecht über diese Daten hat und dass der Verantwortliche für die Anwendung des Datenschutzrechts zuständig ist.

(3) Sollte eine Bestimmung dieser Vereinbarung gleich aus welchem Grund für ungültig, rechtswidrig oder undurchsetzbar befunden werden, wird die betreffende Bestimmung ausgenommen und bleiben die übrigen Bestimmungen dieser Vereinbarung so in vollem Umfang in Kraft und rechtswirksam, als wäre diese Vereinbarung ohne die ungültige Bestimmung geschlossen worden.

MUSTER

Anlage 1 – technisch organisatorische Maßnahmen der DPEPS

Anlage 2 – technisch organisatorische Maßnahmen der DPAG

MUSTER

Anlage 1 - technisch organisatorische Maßnahmen der DPEPS

(1) Vertraulichkeit (Artikel 32 Absatz 1 Buchstabe b DSGVO)

- **Physische Zugangskontrolle**

  Kein unbefugter Zugang zu Datenverarbeitungseinrichtungen, z. B. Magnet- oder Chipkarten, Schlüssel, elektronische Türöffner, Mitarbeiter der Gebäudesicherheitsdienste und/oder für Eingangskontrollen, Alarmsysteme, Videoüberwachungs-Systeme

  Umgesetzte Maßnahmen:

  1. Elektronische Zutrittskontrolle an allen Standorten sowie zusätzlich innerhalb der Standorte für verschiedene Schutzzonen (z.B. Serverräume)
  2. Zutritt für Betriebsfremde und Dienstleister nur nach Authentisierung, Verpflichtung und Begleitung durch interne Mitarbeiter
  3. Einbruchmeldeanlagen sowie optische Zutrittsüberwachung an allen Produktions- und IT-Standorten
  4. Erteilung von Zutrittsgenehmigungen nur durch Leitungskräfte über eine entsprechende Berechtigungsmatrix

- **Elektronische Zugangskontrolle**

  Keine unbefugte Nutzung der Systeme zur Datenverarbeitung und -speicherung, z. B. (sichere) Passwörter, automatische Sperr-/Schließmechanismen, Zwei-Faktoren-Authentifizierung, Verschlüsselung von Datenträgern/Speichermedien

  Umgesetzte Maßnahmen:

  1. Berechtigungskonzept für den Zugang zu allen IT-Systemen
  2. Produktion innerhalb eines gesicherten Virtual Private Network (VPN)
  3. Schutz durch Firewall-Systeme mit Zugang über eine DMZ
  4. Dateneinlieferung nur für autorisierte Einlieferer
  5. Personalisierte Benutzer, Administratorkonten getrennt von Officekonten

- **Interne Zugangskontrolle** (Nutzerrechte für den Zugang zu und die Änderung von Daten)

  Kein unbefugtes Lesen, Kopieren, Ändern oder Löschen von Daten im System, z. B. Berechtigungskonzept, Zugangsrechte auf Need-to-know-Basis, Zugangsprotokollierung

  Umgesetzte Maßnahmen:

  1. Berechtigungskonzept für den Zugang zu allen IT-Systemen
  2. Erteilung zu Zugriffen nach dem „Need to Know Prinzip“

MUSTER

3. Protokollierung von Lesen, Kopieren, Ändern oder Löschen von Daten

- **Trennung nach Zweck**

  Getrennte Verarbeitung von Daten, die für verschiedene Zwecke erhoben werden, z. B. Unterstützung des Verantwortlichen zu mehreren Zwecken, Sandboxing-Technik

  Umgesetzte Maßnahmen:

  1. Serielle Verarbeitung der Kundendaten getrennt nach Kunde und Auftrag
  2. Eindeutige Kennzeichnung

- **Pseudonymisierung** (Artikel 32 Absatz 1 Buchstabe a DSGVO, Artikel 25 Absatz 1 DSGVO)

  Eine Methode/Art, personenbezogene Daten so zu verarbeiten, dass die Daten nur mithilfe zusätzlicher Informationen einer bestimmten betroffenen Person zugeordnet werden können; diese zusätzlichen Informationen sind dabei getrennt zu speichern und mit angemessenen technischen und organisatorischen Maßnahmen zu schützen.

  Umgesetzte Maßnahmen:

  für die Art der angebotenen Dienstleistung nicht relevant

(2) Integrität (Artikel 32 Absatz 1 Buchstabe b DSGVO)

- **Kontrolle der Datenübermittlung**

  Kein unbefugtes Lesen, Kopieren, Ändern oder Löschen von Daten bei deren elektronischer/m Übermittlung oder Transport, z. B. Verschlüsselung, Virtuelle Private Netze (Virtual Private Networks, VPN), elektronische Signaturen

  Umgesetzte Maßnahmen:

  1. Transfer von Daten nur innerhalb eines privaten gesicherten Corporate Network
  2. Protokollierung von Datenübertragungen
  3. Übertagung nur an autorisierte Empfänger

- **Kontrolle der Dateneingabe**

  Überprüfung, ob und von wem personenbezogene Daten in ein Datenverarbeitungssystem eingegeben bzw. in diesem geändert oder gelöscht werden, z. B. Protokolle, Dokumentenmanagement

  Umgesetzte Maßnahmen:

  1. Protokollierung von Lesen, Kopieren, Ändern oder Löschen von Daten

(3) Verfügbarkeit und Belastbarkeit (Artikel 32 Absatz 1 Buchstabe b DSGVO)

- **Verfügbarkeitskontrolle**

MUSTER

Prävention gegen versehentliche(n) oder absichtliche(n) Zerstörung oder Verlust, z. B. Back-up-Strategie (online/offline; vor Ort/außerhalb des Standortes), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldeverfahren und Notfallplanung

Umgesetzte Maßnahmen:

1. Einsatz von Firewall
2. Virenschutz
3. Notfallhandbuch, ständig besetze Notfallrufnummer, Notfallübungen
4. regelmäßige Backups, sichere Aufbewahrung (separater Brandabschnitt)
5. USV

- **Rasche Wiederherstellung** (Artikel 32 Absatz 1 Buchstabe c DSGVO)

  Umgesetzte Maßnahmen:

  1. Virtualisierte IT-Infrastruktur
  2. ausreichend dimensionierte IT-Infrastruktur

(4) Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Artikel 32 Absatz 1 Buchstabe d DSGVO; Artikel 25 Absatz 1 DSGVO)

- **Datenschutzmanagement**

  Der systematische Ansatz zur Sicherstellung der Umsetzung und Einhaltung der gesetzlichen und betrieblichen Anforderungen des Datenschutzes im DPDHL Konzern. Dies beinhaltet wie z. B. Aktualisierung und Ergänzung von Leitfäden und Richtlinien sowie die jährliche Erstellung eines risikobasierten Auditplans.

  Umgesetzte Maßnahmen:

  1. Integriertes Managementsystem – Datenschutz, Informationssicherheit, Qualitäts-, Umwelt-, und Energiemanagement
  2. Regelmäßige Schulung und Sensibilisierung in Datenschutz, Informationssicherheit
  3. Interne Audits

- **Reaktionsmanagement**

  Die Behandlung von Datenschutzvorfälle, die in der erforderlichen Art und Weise bearbeitet und gemeldet werden. Diesbezüglich ist ein Meldeprozess implementiert.

  Umgesetzte Maßnahmen:

  1. zentrale Meldestelle für Sicherheitsvorfälle
  2. abgestimmte Meldewege mit Verantwortlichen

- **Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen** (Artikel 25 Absatz 2 DSGVO)

MUSTER

Die Umsetzung von technischen und organisatorischen Maßnahmen bezüglich Zweckbindung, Erforderlichkeit, Datensparsamkeit, Datenminimierung und Zugangskontrolle.

Umgesetzte Maßnahmen:

1. automatisierte Löschroutinen (Housekeeping)
2. Speicherung auf notwendiges Maß für Verarbeitung beschränkt

- **Auftrags- oder Vertragskontrolle**

  Verarbeitung durch Dritte nach Maßgabe von Artikel 28 DSGVO ausschließlich auf entsprechende Weisungen des Verantwortlichen, z. B. klare und eindeutige vertragliche Vereinbarungen, formalisierte Auftragsverwaltung, strenge Kontrollen bei der Auswahl der Dienstleister, verpflichtende Vorab-Evaluierung, Nachkontrollen zur Überwachung.

  Umgesetzte Maßnahmen:

  1. Auswahl von Dienstleistern im Rahmen von Ausschreibungsverfahren durch zentralen Einkauf der Deutsche Post AG
  2. Abschluss von Auftragsverarbeitungsverträgen
  3. Lieferantenbewertungen
  4. Regelmäßige Lieferantenaudits

MUSTER

Anlage 2 - technisch organisatorische Maßnahmen der DPAG

(1) Vertraulichkeit (Artikel 32 Absatz 1 Buchstabe b DSGVO)

- **Physische Zugangskontrolle**

  Kein unbefugter Zugang zu Datenverarbeitungseinrichtungen, z. B. Magnet- oder Chipkarten, Schlüssel, elektronische Türöffner, Mitarbeiter der Gebäudesicherheitsdienste und/oder für Eingangskontrollen, Alarmsysteme, Videoüberwachungs-Systeme

  Umgesetzte Maßnahmen:

  1. Elektronische Zutrittskontrolle an allen Standorten sowie zusätzlich innerhalb der Standorte für verschiedene Schutzzonen (z.B. Serverräume)
  2. Zutritt für Dienstleister nur nach Authentisierung, Verpflichtung und Begleitung durch interne Mitarbeiter
  3. Erteilung von Zutrittsgenehmigungen nur durch Leitungskräfte über eine entsprechende Berechtigungsmatrix
  4. Verpflichtung der Mitarbeiter auf Vertraulichkeit nach DSGVO und weiterer einschlägiger Gesetze

- **Elektronische Zugangskontrolle**

  Keine unbefugte Nutzung der Systeme zur Datenverarbeitung und -speicherung, z. B. (sichere) Passwörter, automatische Sperr-/Schließmechanismen, Zwei-Faktoren-Authentifizierung, Verschlüsselung von Datenträgern/Speichermedien

  Umgesetzte Maßnahmen:

  1. Schutz durch Firewall-Systeme mit Zugang über eine DMZ
  2. Dateneinlieferung nur für autorisierte Einlieferer
  3. Einsatz von Verschlüsselungsverfahren nach dem Stand der Technik
  4. Passwortrichtlinie (Mindestlänge: 8 Zeichen, Komplexität: Groß,- und Kleinbuchstabe, Sonderzeichen, Ziffer, Verfall: 60 Tage)
  5. Personalisierte Benutzer, Administratorkonten getrennt von Officekonten

- **Interne Zugangskontrolle** (Nutzerrechte für den Zugang zu und die Änderung von Daten)

  Kein unbefugtes Lesen, Kopieren, Ändern oder Löschen von Daten im System, z. B. Berechtigungskonzept, Zugangsrechte auf Need-to-know-Basis, Zugangsprotokollierung

  Umgesetzte Maßnahmen:

MUSTER

1. Berechtigungskonzept für den Zugang zu allen IT-Systemen
2. Erteilung zu Zugriffen nach dem „Need to Know Prinzip“
3. Protokollierung von Lesen, Kopieren, Ändern oder Löschen von Daten

- **Trennung nach Zweck**

  Getrennte Verarbeitung von Daten, die für verschiedene Zwecke erhoben werden, z. B. Unterstützung des Verantwortlichen zu mehreren Zwecken, Sandboxing-Technik

  Umgesetzte Maßnahmen:

  1. Serielle Verarbeitung der Kundendaten getrennt nach Kunde und Auftrag
  2. Eindeutige Kennzeichnung

- **Pseudonymisierung** (Artikel 32 Absatz 1 Buchstabe a DSGVO, Artikel 25 Absatz 1 DSGVO)

  Eine Methode/Art, personenbezogene Daten so zu verarbeiten, dass die Daten nur mithilfe zusätzlicher Informationen einer bestimmten betroffenen Person zugeordnet werden können; diese zusätzlichen Informationen sind dabei getrennt zu speichern und mit angemessenen technischen und organisatorischen Maßnahmen zu schützen.

  Umgesetzte Maßnahmen:

  für die Art der angebotenen Dienstleistung nicht relevant

(2) Integrität (Artikel 32 Absatz 1 Buchstabe b DSGVO)

- **Kontrolle der Datenübermittlung**

  Kein unbefugtes Lesen, Kopieren, Ändern oder Löschen von Daten bei deren elektronischer/m Übermittlung oder Transport, z. B. Verschlüsselung, Virtuelle Private Netze (Virtual Private Networks, VPN), elektronische Signaturen

  Umgesetzte Maßnahmen:

  1. Transfer von Daten nur innerhalb eines privaten gesicherten Corporate Network
  2. Protokollierung von Datenübertragungen
  3. Übertagung nur an autorisierte Empfänger

- **Kontrolle der Dateneingabe**

  Überprüfung, ob und von wem personenbezogene Daten in ein Datenverarbeitungssystem eingegeben bzw. in diesem geändert oder gelöscht werden, z. B. Protokolle, Dokumentenmanagement

  Umgesetzte Maßnahmen:

  Protokollierung von Lesen, Kopieren, Ändern oder Löschen von Daten

MUSTER

(3) Verfügbarkeit und Belastbarkeit (Artikel 32 Absatz 1 Buchstabe b DSGVO)

- **Verfügbarkeitskontrolle**

  Prävention gegen versehentliche(n) oder absichtliche(n) Zerstörung oder Verlust, z. B. Back-up-Strategie (online/offline; vor Ort/außerhalb des Standortes), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldeverfahren und Notfallplanung

  Umgesetzte Maßnahmen:

  1. Einsatz von Firewall
  2. Virenschutz
  3. Notfallhandbuch, ständig besetze Notfallrufnummer, Notfallübungen
  4. regelmäßige Backups, sichere Aufbewahrung (separater Brandabschnitt)
  5. USV

- **Rasche Wiederherstellung** (Artikel 32 Absatz 1 Buchstabe c DSGVO)

  Umgesetzte Maßnahmen:

  1. Virtualisierte IT-Infrastruktur
  2. ausreichend dimensionierte IT-Infrastruktur

(4) Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Artikel 32 Absatz 1 Buchstabe d DSGVO; Artikel 25 Absatz 1 DSGVO)

- **Datenschutzmanagement**

  Der systematische Ansatz zur Sicherstellung der Umsetzung und Einhaltung der gesetzlichen und betrieblichen Anforderungen des Datenschutzes im DPDHL Konzern. Dies beinhaltet wie z. B. Aktualisierung und Ergänzung von Leitfäden und Richtlinien sowie die jährliche Erstellung eines risikobasierten Auditplans.

  Umgesetzte Maßnahmen:

  1. Integriertes Managementsystem – Datenschutz, Informationssicherheit, Qualitäts-, Umwelt-, und Energiemanagement
  2. Regelmäßige Schulung und Sensibilisierung in Datenschutz, Informationssicherheit
  3. Interne Audits

- **Reaktionsmanagement**

  Die Behandlung von Datenschutzvorfälle, die in der erforderlichen Art und Weise bearbeitet und gemeldet werden. Diesbezüglich ist ein Meldeprozess implementiert.

  Umgesetzte Maßnahmen:

MUSTER

1. zentrale Meldestelle für Sicherheitsvorfälle

2. abgestimmte Meldewege mit Verantwortlichen

- **Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen** (Artikel 25 Absatz 2 DSGVO)

  Die Umsetzung von technischen und organisatorischen Maßnahmen bezüglich Zweckbindung, Erforderlichkeit, Datensparsamkeit, Datenminimierung und Zugangskontrolle.

  Umgesetzte Maßnahmen:

  1. automatisierte Löschroutinen (Housekeeping)

  2. Speicherung auf notwendiges Maß für Verarbeitung beschränkt

- **Auftrags- oder Vertragskontrolle**

  Verarbeitung durch Dritte nach Maßgabe von Artikel 28 DSGVO ausschließlich auf entsprechende Weisungen des Verantwortlichen, z. B. klare und eindeutige vertragliche Vereinbarungen, formalisierte Auftragsverwaltung, strenge Kontrollen bei der Auswahl der Dienstleister, verpflichtende Vorab-Evaluierung, Nachkontrollen zur Überwachung.

  Umgesetzte Maßnahmen:

  1. Auswahl von Dienstleistern im Rahmen von Ausschreibungsverfahren durch zentralen Einkauf der Deutsche Post AG

  2. Abschluss von Auftragsverarbeitungsverträgen

  3. Lieferantenbewertungen

  4. Regelmäßige Lieferantenaudits

MUSTER